

Notice of Allowability

Application No.

09/492,273

Examiner

Michael J. Simitoski

Applicant(s)

RANKL, WOLFGANG

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to the amendment of 7/11/2006.
2. ☒ The allowed claim(s) is/are 1-9.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

1. The response of 7/11/2006 was received and considered.
2. Claims 1-9 are pending.
3. Claims 1-9 are allowed.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance with regard to the references of record:

Everett

5. Applicant's response (7/11/2006, p. 4) argues that the references of record do not show chip card *initialization*. Applicant's response argues that Everett merely describes the method of Diffie-Hellman as it is generally applied when chip cards are used in terminals, rather than a chip card initialization method. Applicant's specification discloses that "during initialization, all globally necessary data are transmitted for this purpose and the necessary file structures set up" (p. 1). The instant specification further discloses that in the known methods, "during initialization of the chip card, a secret key needed for data transmission between a processing station and a chip card must be transmitted once in plaintext" (p. 2). Therefore, as none of the references explicitly disclose, within the confines of a physical terminal, employing the claimed key exchange algorithm between a chip card and the terminal to initialize the card, this argument is persuasive.

Schneier and Chen

Art Unit: 2134

6. **Schneier** teaches generating first values/(x, X) for determining the secret initial value/k (page 513, step 1), transmitting parts of the first values/X (page 513, step 1), generating second values/(y, Y) for determining the secret initial value/k' and transmitting parts of the second values/Y (page 513, step 2), determining the secret initial value/k from at least parts of the first values/x and the transmitted parts of the second values/Y (page 513, step 3) and determining the secret initial value/k' from at least parts of the second values/y and the transmitted parts of the first values/X. **Chen** teaches that to initialize a smart card with a master key, the card/chip card is inserted into an initialization terminal/processing station and the key is transferred (col. 4, lines 5-31).

a. Applicant's appeal brief (3/8/2006) argues the references cited in the final rejection. Specifically, on p. 6, it is argued that the Diffie-Hellman key exchange described on p. 513 of the Schneier reference involves communications between separate parties and not between a processing unit and a chip card. Further, on p. 7, it is stated that "the Diffie-Hellman algorithm described on pp. 513-514 of the Schneier reference "corresponds to the method of secret value determination used by the claimed invention, but not as part of an initialization step." On p. 6, it is stated that "Initialization as used in the specification and claims of the instant application refers to the storage of numbers ("secret values") on a card for use in data encrypted and/or key generation. Further, on p. 11, it is argued that Chen discloses chip card initialization, but that Chen discloses "Generally, initialization will be carried out by the private key server at a physically secure location" (col. 4, lines 5-7) and if a physically secure location were provided, one of ordinary skill would not have been motivated to look to the Diffie-Hellman algorithm.

It is noted that Chen defines initialization by disclosing “the keys necessary to establish initial communications must be pre-stored on the card before the card is transferred to the client”.

b. In light of the arguments reiterated in the previous section, it is clear that Schneier discloses a general protocol (Diffie-Hellman) applicable between two processing entities for securely establishing a key at both entities without actually exchanging that key and without sharing a key prior to the protocol. Schneier discloses that “No one listening on the channel can compute that value” (the shared key). Therefore, Schneier is focusing on a situation where the key values need to be exchanged in such a manner that someone could be “listening” to the communication, such as performing key exchange over the Internet (see Appeal brief, p. 8). Chen discloses that chip cards need to be initialized and that this is done by inserting the card into an initialization terminal, but that this is generally performed at a physically secure location. Therefore, one having ordinary skill in the art, at the time the invention was made, would not have been motivated to combine the Schneier and Chen teachings and perform the Diffie-Hellman key exchange algorithm between a card and a terminal in which the card has been inserted to establish the initial key values of the card. Further, even if Schneier were applied to Chen to establish a session key between a user’s card and station for added security during an ATM banking transaction, this would not be an initialization step, as the card is already distributed to the user and initialized.

Art Unit: 2134

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

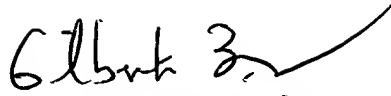
Application/Control Number: 09/492,273

Page 6

Art Unit: 2134



September 25, 2006



GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100